

December 16, 2022

Robert Walker
601.499.8083 (direct)
601.499.8077 (main)
Robert.Walker@WilsonElser.com

Via Electronic Mail: Idtheft@oag.state.md.us

Attorney General Brian Frosh
Office of the Attorney General
Attn: Security Incident Notification
200 St. Paul Place
Baltimore, MD 21202

Re:	Our Client	:	Hawaiian Eye Center
	Matter	:	Data Security Incident
	Wilson Elser File #	:	16516.02012

Dear Attorney Frosh:

We represent Hawaiian Eye Center (“HEC”), with respect to a potential data security incident described in more detail below. HEC takes the security and privacy of the information in its control seriously, and has taken steps to prevent a similar incident from occurring in the future. This letter will serve to inform you of the nature of the security breach, the number of Maryland residents being notified, what information has been compromised, and the steps that HEC is taking to secure the integrity of its systems. We have also enclosed hereto a sample of the notification made to the potentially impacted individuals, which includes an offer of free credit monitoring.

1. Nature of the Security Incident

On November 2, 2022, HEC discovered that one of its servers was not responsive. It was determined that HEC’s network was the victim of a cyber-attack. Upon discovery of the attack, HEC moved quickly to initiate a response, which included shutting down and securing the network. HEC quickly engaged a team of cyber security professionals to conduct a forensic investigation to fully determine the scope and the overall impact of the incident.

After a thorough review of the files potentially obtained by the unauthorized third party, HEC has determined that the following personal information may have been accessed: first name, last name, address, email address, date of birth, Social Security Number, driver’s license, medical records, and health insurance provider and number.

1400 Meadowbrook Road, Suite 100 • Jackson, MS 39211 • p 601.499.8077 • f 601.499.8078

Alabama • Albany • Atlanta • Austin • Baltimore • Beaumont • Boston • Chicago • Dallas • Denver • Edwardsville • Garden City • Hartford • Houston
Indiana • Kentucky • Las Vegas • London • Los Angeles • Miami • Michigan • Milwaukee • Mississippi • Missouri • Nashville • New Jersey • New Orleans
New York • Orlando • Philadelphia • Phoenix • San Diego • San Francisco • Sarasota • Stamford • Virginia • Washington, DC • Wellington • White Plains

wilsonelser.com

As of this writing, HEC has not received any reports of related identity theft since the discovery of the incident

2. Number of Maryland Residents Affected

A total of four (4) Maryland residents were potentially affected by this security incident. Notification letters to potentially impacted individuals were mailed on December 16, 2022, by first class mail. A sample copy of the notification letter is included with this letter.

3. Steps Taken

Immediately upon learning of this incident, HEC contacted a reputable third-party forensic team to assist with its investigation. Since then, HEC has been working with cyber experts to help respond to this incident and review all policies and procedures relating to the security of HEC's systems. HEC is in the process of implementing encryption technologies, updating security management plan, improving physical security, performing updated security risk analysis, revising policies and procedures and training workforce.

Although HEC is not aware of any evidence of misuse of personal information, HEC extended to all potentially impacted individuals an offer for free credit monitoring and identity theft protection through Cyberscout. This service will include 24 months of credit monitoring, along with a fully managed identity theft recovery service, should the need arise.

4. Contact Information

HEC remains dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact me at Robert.Walker@WilsonElser.com or 601-499-8083.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP



Robert Walker, Esq.

RW/ejl

Copy: Erica Lloyd, Esq.
(Wilson Elser LLP)

Enclosure: *Sample Notification Letter*



Via First-Class Mail

[REDACTED]

December 16, 2022

Notice of Data Incident

[REDACTED]

Hawaiian Eye Center (“HEC”) is writing to inform you of an incident that may have exposed your personal information. We take the security of your personal information seriously and apologize for any inconvenience or concern this may cause. You are receiving this letter because you are a current or former patient of HEC. This letter contains additional information about the incident, our response to this incident, and steps you can take to protect yourself.

What Happened and What Information was Involved:

On November 2, 2022, HEC discovered that one of its servers was not responsive. It was determined that HEC’s network was the victim of a cyber-attack. Upon discovery of the attack, HEC moved quickly to initiate a response, which included shutting down and securing the network. We quickly engaged a team of cyber security professionals to conduct a forensic investigation to fully determine the scope and the overall impact of the incident.

After a thorough review of the files potentially obtained by the unauthorized third party, HEC has determined that the following personal information of yours may have been accessed: first name, last name, address, email address, date of birth, Social Security Number, driver’s license, medical records, and health insurance provider and number. As of this writing, HEC has not received any reports of related identity theft since the discovery of the incident.

While we have no evidence that any of your personal information was compromised or misused in any manner, we are taking appropriate precautionary measures to ensure your financial security and help alleviate concerns you may have.

What We Are Doing:

Data security is one of our highest priorities. We value the safety of your personal information. HEC has made immediate enhancements to our systems, security and practices. Additionally, we have engaged appropriate experts to assist us in conducting a full review of our security practices and systems to ensure that enhanced security protocols are in place going forward. We are committed to helping those people who may have been impacted by this unfortunate situation.

In response to the incident, we are providing you with access to the following services:

Representatives are available for 90 days from the date of this letter to assist you with questions regarding this incident between the hours of 8:00 am to 8:00 pm Eastern time, Monday through Friday. Please call the help line 1-800-405-6108 and supply the fraud specialist with your unique code listed below. To extend these services, enrollment in the monitoring services described below is required.

Additionally, we are providing you with access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. These services provide you with alerts for twelve months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services.

How do I enroll for the free services?

To enroll in Credit Monitoring services at no charge, please log on to <https://secure.identityforce.com/benefit/hecinc> and follow the instructions provided. When prompted please provide the following unique code to receive services: [REDACTED] In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

For More Information:

We recognize that you may have questions not addressed in this letter. If you have additional questions, please call 1-800-405-6108, Monday through Friday 8:00 am – 8:00 pm Eastern Time.

HEC values the security of the personal data that we protect, and we apologize for any inconvenience that this incident has caused.

Sincerely,



Steven Rhee, D.O.
Hawaiian Eye Center

Additional Information

Credit Reports: You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at <https://www.consumer.ftc.gov/articles/0155-free-credit-reports>) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze P.O. Box 105788 Atlanta, GA 30348 1-800-349-9960 https://www.equifax.com/personal/credit-report-services/credit-freeze/	Experian Security Freeze P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/freeze/center.html	TransUnion Security Freeze P.O. Box 160 Woodlyn, PA 19094 1-800-909-8872 www.transunion.com/credit-freeze
---	---	--

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with:

- Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf);
- TransUnion (<https://www.transunion.com/fraud-alerts>); or
- Experian (<https://www.experian.com/fraud/center.html>).

A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

File Police Report: You have the right to file or obtain a police report if you experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide proof that you have been a victim. A police report is often required to dispute fraudulent items. You can generally report suspected incidents of identity theft to local law enforcement or to the Attorney General.

FTC and Attorneys General: You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338), TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement. This notice has not been delayed by law enforcement.

For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, and www.oag.state.md.us.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, and www.ncdoj.gov.

For New York residents, the Attorney General may be contacted at Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, and <https://ag.ny.gov/>.

For Rhode Island residents, the Rhode Island Attorney General can be reached at 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident.